# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/003253

International filing date: 22 February 2005 (22.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-053294
Filing date: 27 February 2004 (27.02.2004)

Date of receipt at the International Bureau: 07 April 2005 (07.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/003253

22.02.2005

# 日本国特許庁
# JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月２７日

出願番号
Application Number: 特願２００４－０５３２９４

[ST. 10/C]: ［ＪＰ２００４－０５３２９４］

出願人
Applicant(s): キヤノン株式会社

２００５年　３月２５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２６７５７

【書類名】　特許願
【整理番号】　260413
【提出日】　平成16年 2月27日
【あて先】　特許庁長官殿
【国際特許分類】　B41J 29/38
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　浜田　昇
【特許出願人】
　【識別番号】　000001007
　【氏名又は名称】　キヤノン株式会社
【代理人】
　【識別番号】　100090273
　【弁理士】
　【氏名又は名称】　國分　孝悦
　【電話番号】　03-3590-8901
【手数料の表示】
　【予納台帳番号】　035493
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9705348

【書類名】特許請求の範囲
【請求項１】
ユーザが入力する個人識別コードを受領するコード受領手段と、
乱数を発生させる乱数発生手段と、
前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、
前記受領した個人識別コードを所定の関数で変換するコード変換手段と、
前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と
を有することを特徴とする情報処理装置。
【請求項２】
前記コード変換手段は、前記個人識別コードを一方向関数で変換することを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記コード変換手段は、前記個人識別コードのハッシュ値をとる手段であることを特徴とする請求項２記載の情報処理装置。
【請求項４】
さらに、前記暗号化された乱数、前記変換された個人識別コード、前記暗号化された印刷データを送信する送信手段を有することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
暗号化された乱数、所定関数で変換された第１の個人識別コード、暗号化された印刷データを受信する受信手段と、
ユーザが入力する第２の個人識別コードを受領するコード受領手段と、
前記受領した第２の個人識別コードを所定の関数で変換するコード変換手段と、
前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断手段と、
前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と
、
前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段と
を有することを特徴とする印刷制御装置。
【請求項６】
前記コード変換手段は、前記第２の個人識別コードを一方向関数で変換することを特徴とする請求項５記載の印刷制御装置。
【請求項７】
前記コード変換手段は、前記第２の個人識別コードのハッシュ値をとる手段であることを特徴とする請求項６記載の印刷制御装置。
【請求項８】
さらに、前記復号された印刷データを印刷処理する印刷処理手段を有することを特徴とする請求項５乃至７のいずれか１項に記載の印刷制御装置。
【請求項９】
情報処理装置及び印刷制御装置を含む印刷制御システムであって、
前記情報処理装置は、
ユーザが入力する第１の個人識別コードを受領するコード受領手段と、
乱数を発生させる乱数発生手段と、
前記第１の個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、
前記受領した第１の個人識別コードを所定の関数で変換するコード変換手段と、
前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と、

前記暗号化された乱数、前記変換された第１の個人識別コード、前記暗号化された印刷データを前記印刷制御装置へ送信する送信手段とを有し、

前記印刷制御装置は、

前記暗号化された乱数、前記変換された第１の個人識別コード、前記暗号化された印刷データを前記情報処理装置から受信する受信手段と、

ユーザが入力する第２の個人識別コードを受領するコード受領手段と、

前記受領した第２の個人識別コードを所定の関数で変換するコード変換手段と、

前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断手段と、

前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と、

前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする印刷制御システム。

【請求項１０】

前記情報処理装置及び前記印刷制御装置の前記コード変換手段は、個人識別コードを一方向関数で変換することを特徴とする請求項９記載の印刷制御システム。

【請求項１１】

前記情報処理装置及び前記印刷制御装置の前記コード変換手段は、個人識別コードのハッシュ値をとる手段であることを特徴とする請求項１０記載の印刷制御システム。

【請求項１２】

前記印刷制御装置は、さらに、前記復号された印刷データを印刷処理する印刷処理手段を有することを特徴とする請求項９乃至１１のいずれか１項に記載の印刷制御システム。

【請求項１３】

ユーザが入力する個人識別コードを受領するコード受領ステップと、

乱数を発生させる乱数発生ステップと、

前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化ステップと、

前記受領した個人識別コードを所定の関数で変換するコード変換ステップと、

前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化ステップと

を有することを特徴とする情報処理方法。

【請求項１４】

前記コード変換ステップは、前記個人識別コードを一方向関数で変換することを特徴とする請求項１３記載の情報処理方法。

【請求項１５】

前記コード変換ステップは、前記個人識別コードのハッシュ値をとるステップであることを特徴とする請求項１４記載の情報処理方法。

【請求項１６】

さらに、前記暗号化された乱数、前記変換された個人識別コード、前記暗号化された印刷データを送信する送信ステップを有することを特徴とする請求項１３乃至１５のいずれか１項に記載の情報処理方法。

【請求項１７】

暗号化された乱数、所定関数で変換された第１の個人識別コード、暗号化された印刷データを受信する受信ステップと、

ユーザが入力する第２の個人識別コードを受領するコード受領ステップと、

前記受領した第２の個人識別コードを所定の関数で変換するコード変換ステップと、

前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断ステップと、

前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コ

ード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号ステップと、
前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号ステップと
を有することを特徴とする印刷制御方法。
【請求項１８】
前記コード変換ステップは、前記第２の個人識別コードを一方向関数で変換することを特徴とする請求項１７記載の印刷制御方法。
【請求項１９】
前記コード変換ステップは、前記第２の個人識別コードのハッシュ値をとるステップであることを特徴とする請求項１８記載の印刷制御方法。
【請求項２０】
さらに、前記復号された印刷データを印刷処理する印刷処理ステップを有することを特徴とする請求項１７乃至１９のいずれか１項に記載の印刷制御方法。
【請求項２１】
請求項１３乃至１６のいずれか１項に記載の情報処理方法の各ステップをコンピュータに実行させるためのプログラム。
【請求項２２】
請求項１７乃至２０のいずれか１項に記載の印刷制御方法の各ステップをコンピュータに実行させるためのプログラム。

【書類名】明細書
【発明の名称】情報処理装置、印刷制御装置及び印刷制御システム
【技術分野】
【０００１】
本発明は、例えばパーソナルコンピュータなどの印刷クライアントから、例えばプリンタなどの印刷デバイスにネットワークを介して印刷ジョブを送信する際に、その印刷ジョブデータを途中の盗聴や改ざんから守るために暗号化して送る暗号化印刷技術に関するものである。
【背景技術】
【０００２】
クライアントからネットワークを介して印刷データをプリンタに送って印刷する系においては、経路上で印刷データが盗聴されるあるいは改ざんされるという潜在的な脅威が存在する。
【０００３】
また、プリンタにおいて、従来のように自動的に印刷が開始されて排紙されてしまうのであれば、印刷出力を攻撃者が持ち去ってしまうかもしれないという脅威も存在する。
【０００４】
これらの脅威に対抗するために、ジョブを暗号化して送り、プリンタでは暗号化したまま保持しておき、ユーザがプリンタまで歩いて行ってジョブを確認した後に、そこで始めて復号および印刷を開始するようにシステムを改良する必要がある。
【０００５】
ところが、もしプリンタに複数のジョブが印刷待ちで保持されている場合には、それらのジョブの中から、自分のジョブだけを正しく識別する必要があるが、ジョブ自体が暗号化されているため、全ジョブをスキャンして、ジョブのヘッダ部分に自分のユーザＩＤに相当するものがあるものだけを抜き出すという従来どおりの方法が使えない。
【０００６】
図６は、この問題を概念的に示した模式図である。ホストパーソナルコンピュータ（ＰＣ）１０１および１０５と印刷機能を持つデバイス１０２は、ネットワーク１０４を介して相互に接続されている。今、ホストＰＣ１０１および１０５からデバイス１０２に対して、全部で三つの暗号化印刷ジョブが送られたとする。デバイス１０２では、これらのジョブを印刷することなしに、暗号化した状態のままデバイス１０２内部のジョブ保留領域１０３に保留しておく。
【０００７】
ここで、ホストＰＣ１０１を使っていたあるユーザＡがデバイスの前まで歩いて行って、そこで自分の暗号化印刷ジョブの保留を解いて、印刷を開始させようとするものと仮定する。
【０００８】
ここで問題になるのは、三つのジョブのうちから、どれがユーザＡのジョブかを認識する方法である。
【０００９】
ジョブは暗号化されているから、ジョブのヘッダに埋め込まれているはずのユーザ識別子が一致するものを抜き出すという方法は使えない。ユーザ識別子の部分だけを暗号化しないという方法もあるが、それではユーザＡが印刷を行ったということ自体の秘密が守れず、セキュリティ上好ましくない。
【００１０】
このように、複数のジョブがプリンタに保持されている場合には、正しいジョブを印刷するために、ユーザのジョブを識別するための何らかの方法が必要である。
【００１１】
プリンタで保留状態になっているジョブの識別に関しては、例えば次のような方法が開示されている（例えば特許文献１参照）。

【００１２】
図７は、特許文献１に示された方法を簡単に説明するための概念図である。特許文献１の方法によれば、ホストＰＣ２０１がデバイス２０２に対して印刷データ２１１を送信する。すると、デバイス２０２では、その印刷データを一意に識別する暗証コード２１２を生成し、それをホストＰＣ２０１に送信する。ホストＰＣ２０１側でその暗証コード２１２を受け取ったユーザは、デバイス２０２の前まで移動して、その暗証コード２１２をデバイス２０２に入力することによって、自分のジョブを識別して出力結果を得るというものである。
【００１３】
【特許文献１】特開２００１－１０５６９０号公報
【発明の開示】
【発明が解決しようとする課題】
【００１４】
しかしながら、前記特許文献１の方法では、途中、デバイス側からホスト側へ、暗号化印刷ジョブを守るための番号を通知するという安全でない手順を踏む必要がある。
【００１５】
さらに、特許文献１では、盗聴を防ぐためのジョブの暗号化については触れられておらず、仮に印刷ジョブが暗号化されていたとしても、攻撃者は印刷データの破壊や、あるいはデバイス側で無意味な印刷結果を出力させることによって紙の無駄遣いをさせる事などを目的として、印刷ジョブの改ざんを試みるかもしれない。このような攻撃に対する備えも必要であるが、前記特許文献１では触れられていない。
【００１６】
本発明の目的は、これらの点を改善し、印刷デバイスからホストへジョブを識別するためのＩＤ番号を通知するという安全でない手順を踏む必要を無くし、かつ印刷のセキュリティを保つことである。
【課題を解決するための手段】
【００１７】
本発明の情報処理装置は、ユーザが入力する個人識別コードを受領するコード受領手段と、乱数を発生させる乱数発生手段と、前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、前記受領した個人識別コードを所定の関数で変換するコード変換手段と、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段とを有することを特徴とする。
また、本発明の印刷制御装置は、暗号化された乱数、所定関数で変換された第１の個人識別コード、暗号化された印刷データを受信する受信手段と、ユーザが入力する第２の個人識別コードを受領するコード受領手段と、前記受領した第２の個人識別コードを所定の関数で変換するコード変換手段と、前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断手段と、前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と、前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする。
また、本発明の印刷制御システムは、情報処理装置及び印刷制御装置を含む印刷制御システムであって、前記情報処理装置は、ユーザが入力する第１の個人識別コードを受領するコード受領手段と、乱数を発生させる乱数発生手段と、前記第１の個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化手段と、前記受領した第１の個人識別コードを所定の関数で変換するコード変換手段と、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化手段と、前記暗号化された乱数、前記変換された第１の個人識別コード、前記暗号化された印刷データを前記印刷制御装置へ送信する送信手段とを有し、前記印刷制御装置は、前記暗号化された乱数、前記変換された第１の個人識別コード、前記暗号化された印刷データを前記情報処理装置から受信する

受信手段と、ユーザが入力する第２の個人識別コードを受領するコード受領手段と、前記受領した第２の個人識別コードを所定の関数で変換するコード変換手段と、前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断手段と、前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号手段と、前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号手段とを有することを特徴とする。

また、本発明の情報処理方法は、ユーザが入力する個人識別コードを受領するコード受領ステップと、乱数を発生させる乱数発生ステップと、前記個人識別コード又はそれに基づく鍵を暗号鍵として前記発生させた乱数を暗号化する乱数暗号化ステップと、前記受領した個人識別コードを所定の関数で変換するコード変換ステップと、前記乱数を暗号鍵として印刷データを暗号化する印刷データ暗号化ステップとを有することを特徴とする。

また、本発明の印刷制御方法は、暗号化された乱数、所定関数で変換された第１の個人識別コード、暗号化された印刷データを受信する受信ステップと、ユーザが入力する第２の個人識別コードを受領するコード受領ステップと、前記受領した第２の個人識別コードを所定の関数で変換するコード変換ステップと、前記変換された第１の個人識別コードと前記変換された第２の個人識別コードとが同じか否かを判断する判断ステップと、前記変換された第１及び第２の個人識別コードが同じときには、前記第２の個人識別コード又はそれに基づく鍵を暗号鍵として前記暗号化された乱数を復号する乱数復号ステップと、前記変換された第１及び第２の個人識別コードが同じときには、前記復号された乱数を暗号鍵として前記暗号化された印刷データを復号する印刷データ復号ステップとを有することを特徴とする。

また、本発明のプログラムは、上記の情報処理方法の各ステップをコンピュータに実行させるためのプログラムである。

また、本発明のプログラムは、上記の印刷制御方法の各ステップをコンピュータに実行させるためのプログラムである。

【発明の効果】

【００１８】

印刷制御装置（例えば印刷デバイス）から情報処理装置（例えばホスト）へ印刷データを守るための番号を通知するという安全でない手順を踏むこと無しに、印刷データを暗号化して送ることができ、かつ印刷制御装置側において印刷データの識別も可能になる。また、印刷データを途中で改ざんされる危険を回避することができる。

【発明を実施するための最良の形態】

【００１９】

（第１の実施形態）

図２は、一般的なコンピュータの内部構成を示したものであり、本発明の第１の実施形態のホストＰＣ１０１あるいは印刷デバイス１０２のコントローラも同様の構成を取るものである。

【００２０】

図２において、３００はコンピュータ全体である。コンピュータ３００は、ＲＯＭ３０２あるいは例えばハードディスクなどの大規模記憶装置３１１に記憶されたソフトウェア（コンピュータプログラム）を実行するＣＰＵ３０１を備え、システムバス３０４に接続される各デバイスを総括的に制御する。３１２は、タイマーである。

【００２１】

３０３はＲＡＭで、ＣＰＵ３０１の主メモリ、ワークエリア等として機能する。３０５は外部入力コントローラ（ＫＢＤ　Ｃ）で、コンピュータに備えられた各種ボタンあるいはキーボード３０９等からの指示入力を制御する。３０６はディスプレイコントローラ（ＤＩＳＰＣ）で、表示モジュール（ＤＩＳＰＬＡＹ）３１０の表示を制御する。

【００２２】

記憶装置コントローラ３０７は、ハードディスクなどの大規模記憶装置３１１に対するアクセスを制御する。

【００２３】

３０８はネットワークインタフェースカード（ＮＩＣ）で、ＬＡＮ１０４を介して、他のネットワーク機器あるいはファイルサーバ等と双方向にデータをやりとりする。

【００２４】

図６に、本実施形態の暗号化印刷システムの構成例を示す。ホストＰＣ１０１および１０５と印刷機能を持つ印刷デバイス（プリンタ）１０２は、ネットワーク１０４を介して相互に接続されている。例えば、ホストＰＣ１０１及び／又は１０５がデバイス１０２に対して、３つの暗号化印刷ジョブを送信したとする。デバイス１０２では、これらのジョブを印刷することなしに、暗号化した状態のままデバイス１０２内部のジョブ保留領域１０３に保留しておく。その後、ユーザがデバイス１０２に対して所定の操作を行うことにより、暗号化されたジョブが復号されて印刷される。

【００２５】

図１は、本実施形態における印刷ジョブデータの暗号化方法とジョブの識別方法を示す図である。

【００２６】

ホストＰＣ１０１では、印刷ジョブを暗号化するために、乱数ｒｎｄを発生させ、それをＰＤＬ（ページ記述言語：Page-Description Language）データの暗号鍵として用いる。乱数ｒｎｄは、ユーザが入力したＰＩＮ（個人識別番号：Personal Identification Number）コードをハッシュした値ｋによって暗号化される。値ｋもハッシュされ、後にデバイス１０２側において暗号化ジョブの識別のために用いられる。なお、ＰＩＮは番号以外に文字列を用いたものでもよい。

【００２７】

暗号化されたＰＤＬデータをＣとし、ＰＤＬデータの暗号鍵のハッシュ値ｋをＢとし、乱数ｒｎｄを値ｋで暗号化したものをＡとして、Ａ、ＢおよびＣの三つの組をデバイス１０２側に送信する。

【００２８】

Ａ、ＢおよびＣを受信したデバイス１０２では、ユーザが入力したＰＩＮのハッシュ値を計算し、これをｋ´とする。次にｋ´のハッシュ値を計算し、これをＢ´とする。受信したデータの一部であるＢとＢ´が同一かどうかによって、前記ＰＩＮを入力したユーザのジョブかどうかを判断し、前記ユーザのジョブである場合にはデータを復号して印刷する。

【００２９】

図３は、図１におけるホストＰＣ１０１側におけるジョブの暗号化手順を示したフローチャートである。

【００３０】

図３の手順は、ホストＰＣ１０１上のＣＰＵ３０１によって実行される。さらに前提として、印刷すべき文書や画像等のデータは、プリンタドライバモジュールによってプリンタが読解可能な形式、すなわちＰＤＬデータに変換され、それが図４の手順を実施するモジュールに順次受け渡されるものとする。

【００３１】

印刷データの送出にあたっては、まずステップ５０１において、外部入力コントローラ３０５を制御して、ユーザが入力装置３０９を用いて打ち込むＰＩＮコードを受領する。続くステップ５０２において、乱数ｒｎｄを発生させる。なお、このｒｎｄは、後のステップにおいて、ＰＤＬデータを暗号化するために用いられる。続くステップ５０３において、前記ステップ５０１で受領したＰＩＮコードを基に、ジョブを暗号化するための暗号鍵をさらに暗号化するための暗号鍵ｋを計算する。本実施形態においては、ＰＩＮコードを例えばＭＤ５やＳＨＡ－１などのハッシュ関数に入力し、出力のハッシュ値を暗号鍵ｋとして用いるものとする。続くステップ５０４において、前記ステップ５０３で計算した

値ｋを暗号鍵として、ＰＤＬデータを暗号化するための鍵ｒｎｄを暗号化し、これをＡとする。なお、ＰＩＮコードを暗号鍵としてもよい。続くステップ５０５において、前記ステップ５０３で計算した値ｋのハッシュ値を計算し、これをＢとする。続くステップ５０６において、前記ステップ５０２で発生させた乱数ｒｎｄを暗号鍵として、印刷のためのＰＤＬデータを暗号化し、これをＣとする。続くステップ５０７において、前記ステップ５０４で計算したＡと前記ステップ５０５で計算したＢと前記ステップ５０６で計算したＣを、ＲＡＭ３０３上の一時記憶領域に用意したバッファに格納して送信に備えてひとまとまりにする。続くステップ５０８において、ＮＩＣ３０８を制御して、前記ステップ５０７で用意した送信データをＬＡＮ１０４を介してデバイス１０２に送信する。送信が完了したら、ＲＡＭ３０３上のバッファを解放する。

【００３２】

図４は、図１におけるデバイス１０２側における、ジョブの識別方法と復号手順を示したフローチャートである。デバイス１０２は、ホストＰＣ１０１が送信した上記の送信データを受信する。

【００３３】

図４の手順は、デバイス１０２上のＣＰＵ３０１によって実行される。

デバイスでのジョブの識別と復号にあたっては、まずステップ６０１で、入力コントローラ３０５を制御して、ユーザが入力部３０９を介して入力するＰＩＮコードを受領する。続くステップ６０２で、前記ステップ６０１で受領したＰＩＮコードのハッシュ値ｋ´を計算する。続くステップ６０３で、前記ステップ６０２で計算したｋ´のハッシュ値を計算し、これをＢ´とする。続くステップ６０４において、デバイス１０２内部のジョブ保留領域１０３（図６）に保留されている全ジョブがジョブ識別処理を行われたかどうかを判断する。

【００３４】

もし全ジョブが処理完了されたと判断されたら、本手順を終了する。

もし全ジョブが処理完了されていないと判断されたら、ステップ６０５に進む。ステップ６０５では、処理対象ジョブのヘッダ部分から値Ｂを取り出し、前記ステップ６０３で計算した値Ｂ´と同じかどうかを判断する。

【００３５】

もし同じであると判断されたら、ステップ６０６に進み、ジョブのヘッダ部分から値Ａを取り出して、それを前記ステップ６０２で計算した値ｋ´を暗号鍵として、復号処理を行う。そして得られた値をｒｎｄ´とする。

【００３６】

続くステップ６０７において、ジョブから暗号化されたＰＤＬデータＣを取り出し、それを前記ステップ６０６で計算した値ｒｎｄ´を暗号鍵として、復号処理を行う。そして得られた値が、印刷すべきＰＤＬデータである。続くステップ６０８では、前記ステップ６０７で得たＰＤＬデータを印刷処理する。

【００３７】

ステップ６０８の処理が終了したら、あるいはステップ６０５においてＢとＢ´が同じではないと判断された場合には、ステップ６０４に戻り、次のジョブに対して処理を続行する。

【００３８】

上記で説明した本実施形態に係るホストＰＣ１０１あるいはデバイス１０２のプログラムは、外部からインストールされるプログラムによって、ホストＰＣ１０１あるいはデバイス１０２によって実行されても良い。その場合、そのプログラムはＣＤ－ＲＯＭやフラッシュメモリやフレキシブルディスクなどの記憶媒体により、あるいは電子メールやパソコン通信などのネットワークを介して、外部の記憶媒体からプログラムを含む情報群をホストＰＣ１０１あるいはデバイス１０２上にロードすることにより、ホストＰＣ１０１あるいはデバイス１０２に供給される場合でも本発明は適用されるものである。

【００３９】

図５は、記憶媒体の一例であるＣＤ－ＲＯＭのメモリマップを示す図である。９９９９はディレクトリ情報を記憶してある領域で、以降のインストールプログラムを記憶してある領域９９９８および印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域９９９７の位置を示している。９９９８は、インストールプログラムを記憶してある領域である。９９９７は、印刷クライアントあるいはネットワークプリンタの制御プログラムを記憶してある領域である。本実施形態の印刷クライアントあるいはネットワークプリンタの制御プログラムがホストＰＣ１０１あるいはデバイス１０２にインストールされる際には、まずインストールプログラムを記憶してある領域９９９８に記憶されているインストールプログラムがシステムにロードされ、ＣＰＵ３０１によって実行される。次に、ＣＰＵ３０１によって実行されるインストールプログラムが、デバイス制御プログラムを記憶してある領域９９９７から印刷クライアントあるいはネットワークプリンタの制御プログラムを読み出して、ＲＯＭ３０２の内容を書き換えるか、あるいは大規模記憶装置３１１にインストールする。この場合、ＲＯＭ３０２は単純なマスクＲＯＭではなく、フラッシュＲＯＭなどの書き換え可能なＲＯＭである必要がある。

【００４０】

なお、本実施形態は、複数の機器（例えばホストコンピュータ、インタフェース機器、リーダなど）から構成されるシステムあるいは統合装置に適用しても、ひとつの機器からなる装置に適用してもよい。

【００４１】

また、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読み出し実行することによっても、本発明の目的が達成されることは言うまでもない。

【００４２】

この場合、記憶媒体から読み出されたプログラムコード自体が本発明の新規な機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００４３】

プログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどを用いることができる。

【００４４】

また、コンピュータが読み出したプログラムコードを実行することによって、前述した実施形態の機能が実現される他、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【００４５】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によっても前述した実施形態の機能が実現され得る。

【００４６】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体から、そのプログラムをパソコン通信など通信ラインを介して要求者にそのプログラムを配信する場合にも適用できることは言うまでもない。

【００４７】

（第２の実施形態）

本発明の第２の実施形態を説明する。第１の実施形態では、ＰＤＬデータを暗号化するための暗号鍵ｒｎｄを、さらに暗号化するための鍵として、ユーザが入力したＰＩＮコー

ドをハッシュした値を用いたが、特にこの方法に限るものではなく、ＰＩＮコードを基にした一方向性関数で、変換された後の値の一致性が確認できるものであれば何でも良い。

【００４８】

例えば、ハッシュを計算する回数を一回ではなく、出力結果をさらにハッシュ関数に入力して二回ハッシュをかける方法でも良いし、ある決まった数とＰＩＮコードとのＸＯＲを取って、それのハッシュ値を得ることを複数回繰り返すということでも良い。

【００４９】

当然、これらの場合には、デバイス側でジョブを識別するにあたって、ＰＩＮを扱う方法を、ホストＰＣ側で用いた方法と同様の方法にする必要がある。

【００５０】

以上のように、第１及び第２の実施形態では、ホスト側において、ユーザが入力するＰＩＮコードを受け取る手段と、乱数を発生させる手段と、前記発生させた乱数を暗号化する手段と、前記受け取ったＰＩＮコードを容易に推測することができない値に変換する手段と、印刷ジョブデータを暗号化する手段とをもたせる。

【００５１】

さらに、デバイス側において、ユーザが入力するＰＩＮコードを受け取る手段と、受信した暗号化ジョブの真正性を確認する手段と、暗号化ジョブの暗号鍵を計算する手段と、暗号化ジョブを復号する手段とを持たせる。

【００５２】

デバイスからホスト側へ印刷ジョブを守るための番号を通知するという安全でない手順を踏むこと無しに、印刷データを暗号化して送ることができ、かつデバイス側においてジョブの識別も可能になる。また、印刷データを途中で改ざんされる危険も回避することができる。すなわち、ジョブを識別するためのＩＤを乱数値で自動生成し、かつその乱数値を暗号化するなど、改ざん検知を含めてセキュリティを保つことができる。

【００５３】

なお、上記実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【図面の簡単な説明】

【００５４】

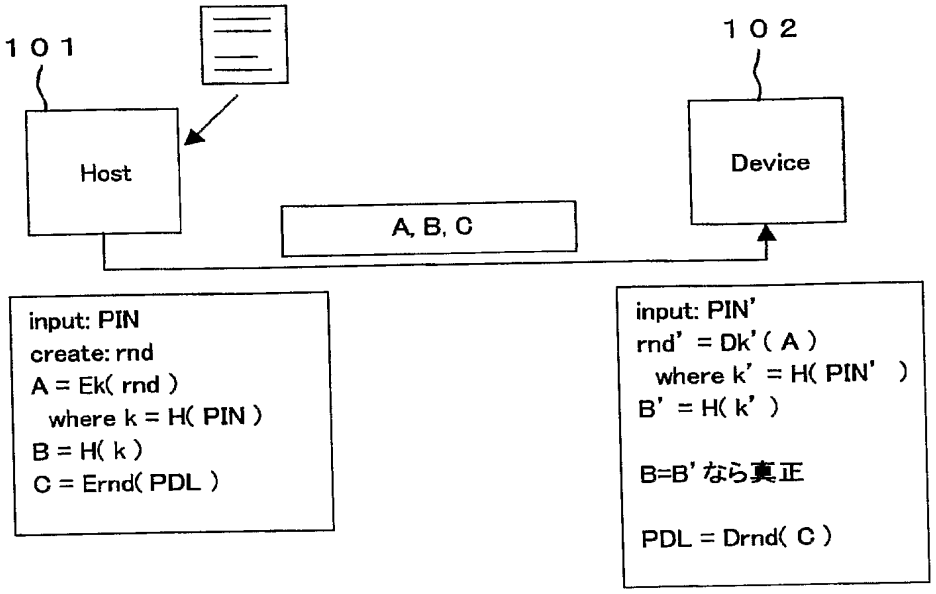
【図１】実施形態の暗号化印刷方法の仕組みを示す図である。
【図２】実施形態のホストＰＣあるいは印刷デバイスの内部構成を示す図である。
【図３】実施形態におけるホストＰＣの動作を示すフローチャートである。
【図４】実施形態における印刷デバイスの動作を示すフローチャートである。
【図５】実施形態のソフトウェアの記憶媒体におけるメモリマップを示す図である。
【図６】暗号化印刷におけるジョブ識別問題を示す概念図である。
【図７】従来技術におけるジョブ識別方法の一例を示す図である。

【符号の説明】

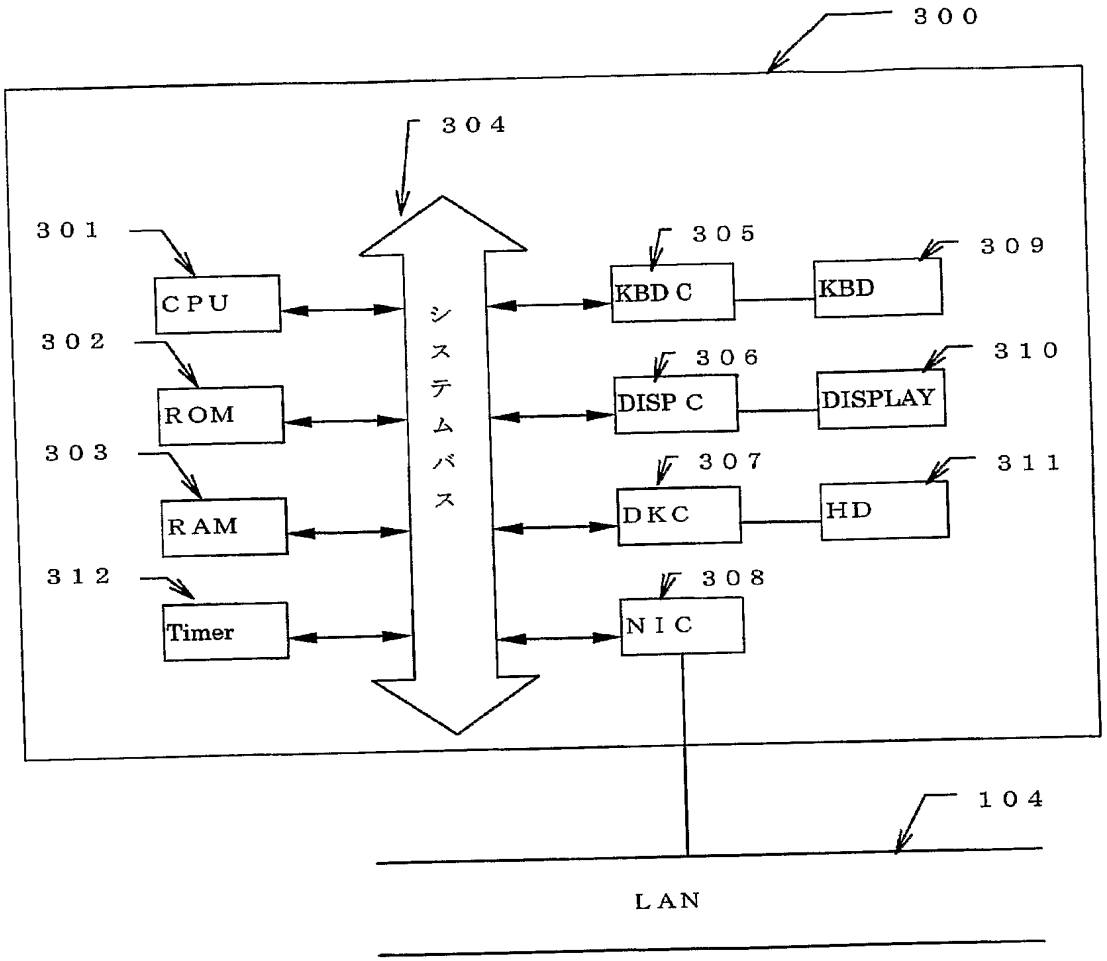
【００５５】

３０９、５０１、６０１　ＰＩＮコード受領手段
５０２　乱数発生手段
５０４　乱数暗号化手段
５０３、５０５、６０２、６０３　ＰＩＮコード変換手段
５０６　印刷データ暗号化手段
６０５　ジョブ識別手段
６０６　暗号鍵計算手段
６０８　印刷データ復号化手段

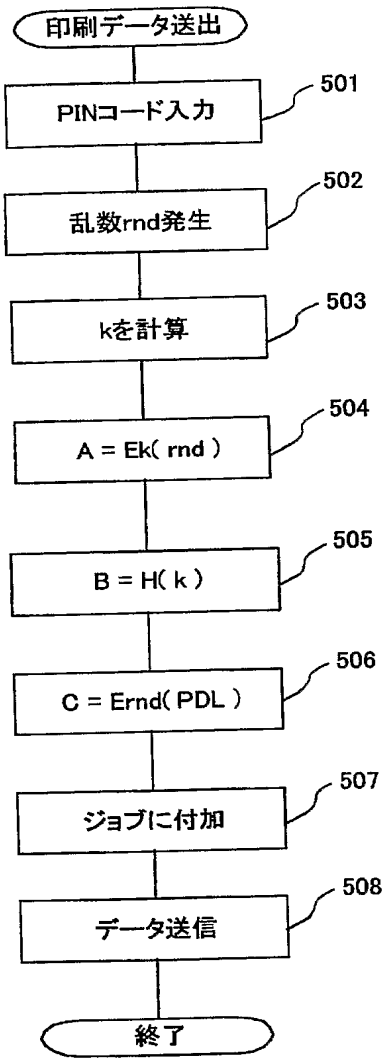
【書類名】図面
【図１】


１０１
１０２
Host
Device
A, B, C
input: PIN
create: rnd
A = Ek( rnd )
where k = H( PIN )
B = H( k )
C = Ernd( PDL )
input: PIN'
rnd' = Dk'( A )
where k' = H( PIN' )
B' = H( k' )
B=B' なら真正
PDL = Drnd( C )

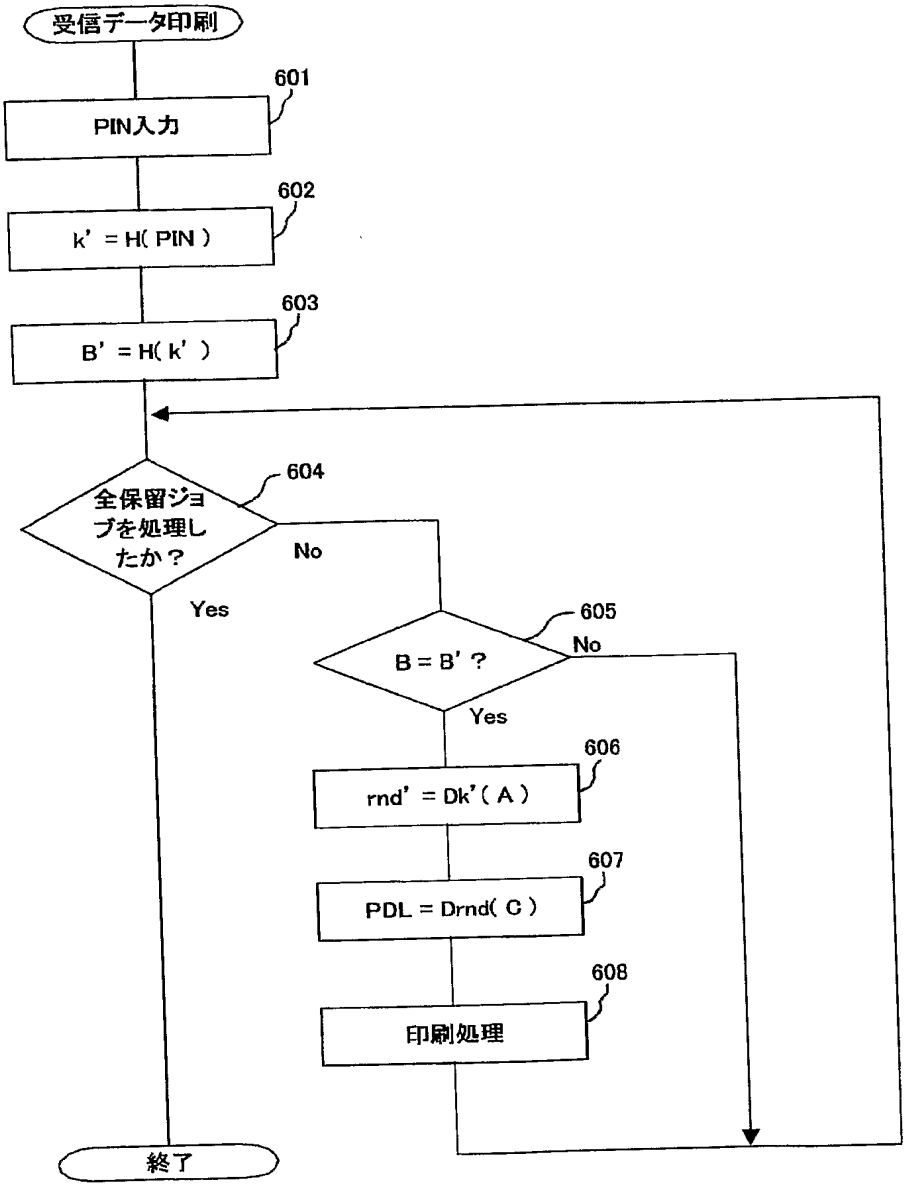
【図２】


300
304
301
CPU
302
ROM
303
RAM
312
Timer
システムバス
305
KBD C
309
KBD
306
DISP C
310
DISPLAY
307
DKC
311
HD
308
NIC
104
LAN

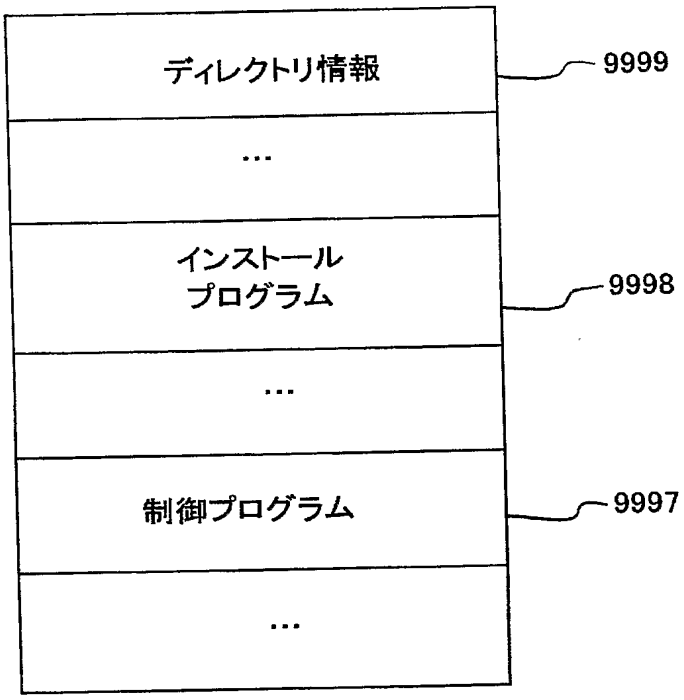
【図３】


印刷データ送出
PINコード入力
501
乱数rnd発生
502
kを計算
503
A = Ek( rnd )
504
B = H( k )
505
C = Ernd( PDL )
506
ジョブに付加
507
データ送信
508
終了

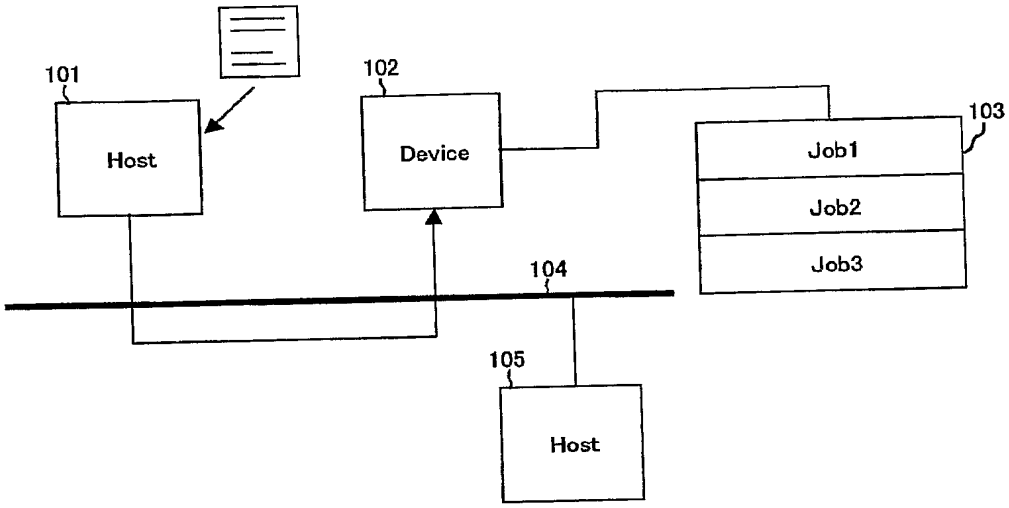
【図４】


受信データ印刷
601
PIN入力
602
k' = H( PIN )
603
B' = H( k' )
604
全保留ジョブを処理したか？
No
Yes
605
B = B' ?
No
Yes
606
rnd' = Dk'( A )
607
PDL = Drnd( C )
608
印刷処理
終了

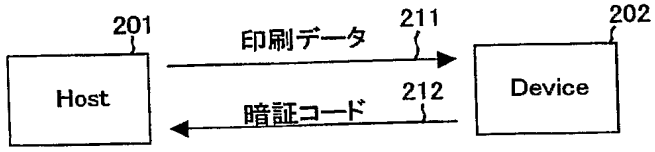
【図５】



【図６】


101
Host
102
Device
103
Job1
Job2
Job3
104
105
Host

【図７】


201
Host
印刷データ
211
212
暗証コード
202
Device

【書類名】要約書
【要約】
【課題】　印刷デバイスからホストへジョブを識別するためのＩＤ番号を通知するという安全でない手順を踏む必要を無くし、かつ印刷のセキュリティを保つことを課題とする。
【解決手段】　ユーザが入力する個人識別コード（ＰＩＮ）を受領するコード受領手段と、乱数（ｒｎｄ）を発生させる乱数発生手段と、個人識別コード又はそれに基づく鍵を暗号鍵として発生させた乱数を暗号化する乱数暗号化手段と、受領した個人識別コードを所定の関数で変換するコード変換手段と、乱数を暗号鍵として印刷データ（ＰＤＬ）を暗号化する印刷データ暗号化手段とを有する情報処理装置が提供される。
【選択図】　図１

特願２００４－０５３２９４

出　願　人　履　歴　情　報

識別番号　［０００００１００７］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社